Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Comment Sought on Privacy and Security of Information Stored on Mobile Communications Devices	)	CC Docket No. 96-115
	)	
	)	DA 12-818
	)	

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200

July 13, 2012

TABLE OF CONTENTS

PAGE

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Comment Sought on Privacy and Security of Information Stored on Mobile Communications Devices	)	CC Docket No. 96-115
	)	
	)	DA 12-818
	)	

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

I. INTRODUCTION AND SUMMARY

CTIA – The Wireless Association® ("CTIA") hereby respectfully submits its comments in response to the Commission's Public Notice in the above-captioned proceeding.[1] The Public Notice seeks comment on mobile wireless service providers' practices regarding network diagnostic information stored on mobile communications devices. Specifically, the Commission inquires about "the applicability . . . in this context of telecommunications carriers' duty under section 222(a) to protect customer information," suggesting that the information at issue "on its face" qualifies as "customer proprietary network information" ("CPNI").

CTIA wholeheartedly supports the goal of protecting the privacy and security of customer information stored on mobile communications devices. CTIA also appreciates the Commission's recognition that network diagnostic tools "may be a legitimate and effective way to improve the quality of wireless service."[2] Carriers are always striving to provide the most reliable wireless voice and data service for their customers. Carriers may know that calls are being dropped or that a specific geographic area has poor reception, but they do not always know

---

[1] *Comment Sought On Privacy And Security Of Information Stored On Mobile Communications Devices,* Public Notice, CC Docket No. 96-115, DA 12-818 (May 25, 2012) ("Public Notice").

[2] *Id.* at 1.

why a call drops, why a website fails to load, why a text message was not timely delivered, or why service is unavailable in a particular area.[3] Network diagnostic tools enable carriers to resolve these problems and provide better service to their subscribers. Network diagnostic software is an invaluable type of such network diagnostic tool,[4] allowing wireless providers to better understand how mobile devices interact with and perform on their networks.[5] Indeed, the Commission has acknowledged that many wireless carriers use such software to identify service issues and ultimately solve them.[6] Consumers are well aware of this practice because carriers clearly and conspicuously disclose that they gather this type of information to improve network performance and the user's experience.

CTIA cautions the Commission not to adopt new rules under Section 222 that would limit wireless carriers' use of network diagnostic tools to improve wireless voice and data service. Such rules are unnecessary and would actually harm consumers by hamstringing providers in their ability to improve service quality, especially in these times of wireless spectrum capacity constraints. More broadly, regulating data stored on mobile devices in today's "Open Internet" environment would be ineffective and counterproductive. Wireless carriers no longer control—or even know—the third parties that create software and install it on wireless devices or the data associated with these applications. Wireless carriers today are not gatekeepers for wireless customers. Accordingly, the Commission should not, as a matter of regulatory policy, adopt any

---

3 Letter from Vonya B. McCann, Senior Vice President, Government Affairs, Sprint Nextel, to The Honorable Al Franken, United States Senate, at 1 (Dec. 14, 2011) ("Sprint Letter").

4 Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T Services, Inc., to The Honorable Al Franken, United States Senate, at 1 (Dec. 14, 2011) ("AT&T Letter"); Sprint Letter at 2.

5 Carrier IQ, Understanding Carrier IQ Technology: What Carrier IQ Does and Does Not Do, at 2 (Dec. 15, 2011) ("CIQ Report").

6 Public Notice at 2.

new rules in this area because industry-wide best practices and codes of conduct are the best way to address any perceived problem.

More fundamentally, however, the Commission lacks statutory authority to regulate carriers' use of tools to diagnose and troubleshoot network problems in order to improve the provision of service to subscribers. That is so because data stored on mobile devices is *not* CPNI within the meaning of Section 222 because it is not "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."[7] Section 222 does not grant the Commission a roving mandate to safeguard the privacy of all types of data stored on wireless devices, such as text messages, pictures, and emails. Finally, the Stored Communications Act ("SCA") confirms the lack of Commission authority in this area because it gives wireless providers broad authority to access and use their customers' information for network diagnostic purposes.

For these reasons, the Commission should not—indeed, it cannot—adopt any new rules to regulate the privacy and security of information stored on mobile communications devices, or the collection and use of network diagnostic information.

II. REGULATION OF DATA STORED ON MOBILE DEVICES WOULD BE INAPPROPRIATE AS A MATTER OF REGULATORY POLICY.

The Commission should not, as a matter of policy, attempt to regulate the storage of customer data on mobile devices. Any effort to regulate in this area would be ineffective in today's environment and counterproductive to the Commission's Open Internet goals. Moreover, as the Commission has recognized, wireless carriers need flexibility to use stored data for network diagnostic purposes for the ultimate good of improving wireless service. NTIA is already considering these privacy issues as part of a broader, ongoing multi-stakeholder process

[7] 47 U.S.C. § 222(h)(1).

that involves the wireless industry. The Commission should not attempt to get out ahead of this process.

Regulating the practices of network providers would be an ineffective way to protect consumer privacy because many other entities in the wireless space have access to personal data stored on mobile devices. Due to the openness of the Internet, today's privacy risks originate from the acts and omissions of entities independent of the carrier-customer relationship. Indeed, consumers use a variety of applications and other third-party software to store personal data on their mobile devices, providing many other players in the wireless ecosystem with the ability to access this information. Wireless carriers have no control over these third parties and are unable to restrict their access to consumer information residing on a mobile device. The Commission's CPNI rules address a fundamentally different problem from those that consumers face today in an Open Internet environment. The Commission should not use its CPNI rules to impose gatekeeper obligations on network providers because any such rules would be ineffective.

Relatedly, regulating wireless carriers in this area would be counterproductive to the Commission's Open Internet policies. Third-party access to and use of this stored data results from the very Open Internet the Commission advocates. Regulating this data would run counter to consumers' demand for the same latitude to install third-party software, services, and applications on their mobile devices that they enjoy on their home computers. Indeed, in today's world, smartphones are fundamentally computing devices. Just as a broadband Internet service provider may be unable to access data stored on their customers' home computer, the wireless network provider is similarly constrained vis-à-vis the user's smartphone. Carriers provide their consumers with wide latitude to download apps and software that may access their data, and

wireless users have the same expectations for their mobile devices. This is precisely the Open Internet environment the Commission has encouraged.

Moreover, as the Commission has acknowledged,[8] there are many acceptable uses of data stored on mobile devices. Most notably, wireless carriers use network diagnostic information stored on mobile devices to improve wireless voice and data service. These tools ultimately benefit consumers, and their use should not be discouraged by the Commission. Restricting or forbidding the use of these tools would harm consumers by hamstringing providers in their ability to improve service quality with the limited spectrum capacity currently available.

In today's multi-player environment, flexibility is key. Wireless carriers require the flexibility that industry-wide best practices and codes of conduct can provide. The Commission should allow the industry to develop these best practices that lead the way in this area. The Commission should not get out ahead of industry best practices with misguided regulation that could squash these stakeholder efforts and, despite the very best of intentions, inadvertently cast in stone rules for such rapidly evolving technologies and services.

Indeed, NTIA has already started the type of multi-stakeholder process that is best suited to address the issues in this Public Notice. All players in the wireless ecosystem will be involved in the development of comprehensive and consistent solutions that will address consumers' expectations across a broad range of applications. Wireless providers will be actively engaged in that process. The concerns the FCC raises are a small subset of a broader, more complex issue—namely, how to best protect consumers in an Open Internet environment. Consumers need consistent privacy protections across the board, without regard to the type of technology or company that collects or uses the data. The Commission should await the result of this process

[8] Public Notice at 1.

before adopting any new rules in this area that could inadvertently harm the very consumers it seeks to protect.

III. SECTION 222 DOES NOT AUTHORIZE THE COMMISSION TO REGULATE WIRELESS PROVIDERS WHEN THEY RETRIEVE INFORMATION STORED ON WIRELESS DEVICES BECAUSE SUCH INFORMATION IS NOT CPNI.

Section 222 of the Act requires "telecommunications carriers" to protect "customer proprietary network information" to the extent they acquire this information by providing "telecommunications services."[9] Under Section 222, "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, . . . customers."[10] "Section 222 sets forth three categories of customer information to which different privacy protections and carrier obligations apply—individually identifiable CPNI, aggregate customer information, and subscriber list information."[11] "Congress accorded CPNI—which includes personal, individually identifiable information—the greatest level of protection."[12]

Congress also provided a specific definition for that term. Under Section 222, CPNI is "information that relates to the quantity, technical configuration, type, destination, location, and

---

[9] Even if information stored on mobile devices qualifies as CPNI, it is not regulated under Section 222 to the extent it is obtained by virtue of the provision of an information service. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, ¶ 1 (1998) ("*1998 CPNI Order*") ("Section 222 establishes a new statutory framework governing carrier use and disclosure of customer proprietary network information (CPNI) and other customer information obtained by carriers *in their provision of telecommunications services*." (emphasis added)); *see also* 47 U.S.C. § 222(c)(1), (3) (restricting use of CPNI obtained "by virtue of [the] provision of a telecommunications service").

[10] 47 U.S.C. § 222(a); 47 C.F.R. § 64.2010(a).

[11] *1998 CPNI Order* ¶ 2.

[12] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, ¶ 7 (2002) ("*2002 CPNI Order*").

amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, *and* that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[13] The Commission has explained that "CPNI includes information that is extremely personal to customers as well as commercially valuable to carriers, such as to whom, where and when a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent the service is used.[14] "Practically speaking, CPNI includes personal information such as the phone numbers called by a consumer, the length of phone calls, and services purchased by the consumer, such as call waiting."[15]

Network diagnostic information and other information acquired from wireless devices is not CPNI because it does not contain personally identifiable call data.[16] As explained above, network diagnostic software supplies wireless carriers with information about the functionality and performance of the device in relation to the provider's wireless network. This information concerns the problems that wireless consumers typically have with their mobile devices and the network—dropped calls, failed data sessions, poor battery performance, poor signal strength,

---

13 47 U.S.C. § 222(h)(1) (emphasis added); *see also* 47 C.F.R. §§ 64.2001-.2011.

14 *1998 CPNI Order* ¶ 2.

15 *2002 CPNI Order* ¶ 7; *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, ¶ 5 (2007) ("*2007 CPNI Order*").

16 *See* Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 22 (July 9, 2007).

frozen or failed applications, and dead zones.[17] This can include data on when and where calls fail; the locations where customers have problems accessing the network; the reliability and battery performance of their make and model of device; and the interaction of the mobile network with the mobile device—known as network signaling traffic.[18] Network diagnostic software frequently collects the location, date, and time a handset experiences a network event, such as a dialed or received telephone call, a dropped call or an attempted call when the handset has no signal.[19] The underlying analytical data for a dropped call, for instance, could include the signal strength of the cell towers in a particular area for a random volume of calls.[20] Other analytical data can include network performance, battery life, ability and speed to access a website, and the usage, performance and stability of an application.[21]

Once wireless carriers obtain this information, they use it only to diagnose and troubleshoot problems in order to improve the network and customer service.[22] Wireless carriers have clearly stated that they do not use network diagnostic software to obtain the contents of customers' communications or online search queries, to look at photos, video or voice messages, to track where their customers go on the Internet or their location, to collect the names or contact

---

17 AT&T Letter at 2; Letter from Thomas J. Sugrue, Senior Vice President, Regulatory and Legal Affairs, T-Mobile USA, Inc., to The Honorable Al Franken, United States Senate, at 1-2 (Dec. 20, 2011) ("T-Mobile Letter").

18 CIQ Report at 2.

19 AT&T Letter at 1.

20 Sprint Letter at 2.

21 CIQ Report at 3.

22 *See* CIQ Report at 10; AT&T Letter at 1 (AT&T uses Carrier IQ "*only* to collect diagnostic information about its network."); Sprint Letter at 1 (Sprint does not use "the data collected using Carrier IQ software beyond . . . 'technical diagnostics information'"); T-Mobile Letter at 2 ("T-Mobile collects this type of technical data solely to understand what is happening on the device and the network so that we can more effectively and directly troubleshoot issues with dropped calls, failed applications, signal strength and roaming, or battery and device performance that might negatively impact our customers' experience and satisfaction.").

information in users' address books, or to gather keystroke data.[23] Put simply, network diagnostic information and other data stored on wireless devices does not relate "to whom, where and when a customer places a call" or the "services purchased by the customer."[24]

For these reasons, the information at issue does not "relate[] to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier," and thus does not meet the statutory definition of CPNI. Accordingly, it does not matter whether the information is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[25] Section 222 uses the conjunctive term "and," meaning *both* elements of the definition thus must be met.[26] In sum, Section 222 does not apply to the storage and retrieval of network diagnostic information.[27]

Finally, to the extent the Public Notice seeks to broadly regulate data stored on mobile devices,[28] it exceeds the reach of the Commission's authority under Section 222. Consumers create and store all types of personal data on their mobile phones—from emails and texts to

---

23 AT&T Letter at 1, 3; Sprint Letter at 2, 3; T-Mobile Letter at 2.

24 *1998 CPNI Order* ¶ 2.

25 *Cf*. Public Notice at 4.

26 *See* Norman J. Singer and J.D. Shambie Singer, 1A Sutherland Statutory Construction § 21:14 (7th ed.) (explaining that use of "the conjunctive 'and'" indicates "legislative intent that all of the requirements must be fulfilled to comply with the statute").

27 Even if this information were CPNI, Section 222 and the Commission's implementing rules would clearly permit wireless providers to use it in order to improve wireless service. 47 U.S.C. § 222(c)(1), (c)(3); 47 C.F.R. § 64.2005(b)(1); 47 C.F.R. § 64.2005(c)(1); 47 C.F.R. § 64.2005(d). As the Commission has explained, "customer approval for carriers to use, disclose, and permit access to CPNI can be inferred in the context of an existing customer-carrier relationship. This is so because the customer is aware that its carrier has access to CPNI, and, through subscription to the carrier's service, has implicitly approved the carrier's use of CPNI within that existing relationship." *1998 CPNI Order* ¶ 23.

28 *See* Public Notice at 4 (inquiring "into practices of mobile wireless service providers with respect to information stored on their customers' mobile communications devices").

pictures and tweets. None of this data meets Congress' definition of CPNI because none contains personally identifiable call data.[29] For the Commission to exercise regulatory control over any and all types of data stored by consumers on mobile devices would flip Section 222 on its head by allowing the Commission to intrude into consumer conduct to an unprecedented degree—under the guise of protecting consumer privacy. Moreover, Congress simply has not conferred upon the Commission a roving mandate in Section 222 to regulate the privacy of all other types of data on consumers' mobile devices.

IV. THE STORED COMMUNICATIONS ACT PROVIDES WIRELESS PROVIDERS WITH INDEPENDENT AUTHORITY TO EXAMINE NETWORK DIAGNOSTIC INFORMATION STORED ON WIRELESS DEVICES.

The Stored Communications Act confirms that the Commission lacks statutory authority to regulate wireless carriers' use of network diagnostic information. "[T]he meaning of one statute may be affected by other Acts, particularly where Congress has spoken subsequently and more specifically to the topic at hand."[30] Here, Congress has conferred upon wireless providers express statutory immunity to access and use their customers' network diagnostic information in order to improve wireless service.

The SCA explicitly states that communications providers "may divulge a record or other information pertaining to a subscriber or customer of such service . . . with the lawful consent of the customer or subscriber" or "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service" or "to any person other

---

[29] 47 U.S.C. § 222(h)(1) (defining CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier").

[30] *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000); *see also Am. Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005) ("[S]ubsequent legislation enacted by Congress *confirms* the limited scope of the agency's ancillary jurisdiction.").

than a governmental entity."[31] Wireless customers "consent" to the collection and use of network diagnostic information when they sign up for wireless service because carriers disclose in their privacy policies that they collect and use this information to improve wireless service.[32] The use of this information is further authorized because it is "necessarily incident to the rendition of" wireless voice and data service and is not provided to the Government.

The Commission has no power to strip wireless providers of rights granted by Congress in other federal laws. Under the APA, the Commission is prohibited from taking action that is "not in accordance with law."[33] The phrase "not in accordance with law means, of course, *any* law, and not merely those laws that the agency itself is charged with administering."[34] Thus, the Commission would act unlawfully by issuing CPNI rules and regulations that conflict with "another federal law,"[35] such as the SCA.

---

[31] 18 U.S.C. § 2702(c)(2), (3), (6). Although Section 2702(c) is titled as an "Exception" to Section 2702(a), wireless carriers' use of network diagnostic information does not fall within the prohibitions in Section 2702(a) for a variety of reasons, not least of which is that wireless carriers do not provide this information to the Government.

[32] *See* AT&T Letter at 5-6; T-Mobile Letter at 5-6; Sprint Letter at 4-5; Verizon, Privacy Policy, *available at* http://www22.verizon.com/privacy/; *see also Mortensen v. Bresnan Communication, L.L.C.*, 2010 WL 5140454, at *4-5 (D. Mont. Dec. 13, 2010) (dismissing claims under 18 U.S.C. § 2511(2)(d) because plaintiffs consented to interception disclosed in online privacy notice and subscriber agreement); *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) ("The legislative history shows that Congress intended the consent requirement [of ECPA] to be construed broadly. . . . Consent may be express or implied.").

[33] 5 U.S.C. § 706(2).

[34] *FCC v. NextWave Personal Commc'ns, Inc.*, 537 U.S. 293, 300 (2003) (emphasis in original).

[35] *NextWave Personal Commc'ns, Inc. v. FCC*, 254 F.3d 130, 149 (D.C. Cir. 2001), *aff'd* 537 U.S. 293; *see also Scheduled Airlines Traffic Offices, Inc. v. Dept. of Def.*, 87 F.3d 1356, 1361-62 (D.C. Cir. 1996) (holding Department of Defense policy invalid under 5 U.S.C. § 706(2)(A) because it "violated the Miscellaneous Receipts statute"); *Cousins v. Sec'y of the U.S. Dep't of Transp.*, 880 F.2d 603, 608 (1st Cir. 1989) (en banc) ("These words [in Section 706(2)(A)] are general in their meaning; they do not restrict the courts to consideration of the agency's own enabling statute.") (Breyer, J.).

V. CONCLUSION

CTIA and its members share the Commission's concern for the confidentiality of true CPNI. CTIA members take security and privacy seriously and are committed to protecting personalized customer information. However, the Commission should not adopt any new rules that would restrict wireless carriers' ability and legitimate right to use network diagnostic software to collect information that will improve wireless voice and data services. Not only would such rules be unnecessary and actually harm consumers by hamstringing providers in their ability to improve service quality, but the Commission simply lacks statutory authority to regulate in this area.

Respectfully submitted,

By: *Krista L. Witanowski*

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA – The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200

Dated: July 13, 2012